IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Inventor(s):	Hung-Hsiang Jonathan Chao et al.		
Case:	Chao 1-77-1-14 (LCNT/126091)		
Serial No.:	10/723,450	**Group Art Unit:**	2132
Filed:	11/26/2003	**Confirmation #:**	5965
Examiner:	Kane, Cordelia P		
Title:	DISTRIBUTED ARCHITECTURE FOR STATISTICAL OVERLOAD CONTROL AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS		

MAIL STOP AMENDMENT
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

RESPONSE AMENDMENT

In response to the non-final Office Action mailed November 20, 2007, please reconsider the above-identified patent application as follows.

In the event that an extension of time is required for this amendment to be considered timely, and a petition therefor does not otherwise accompany this amendment, any necessary extension of time is hereby petitioned for.

The Commissioner is authorized to charge any fees due, including extension of time and excess claim fees, to counsel's Deposit Account No. 20-0782/LCNT/**126091**.

IN THE SPECIFICATION:

Please amend paragraph [0008] (page 2, line 26 – page 3, line 2) of the specification as follows:

The disadvantages heretofore associated with the prior art are overcome by the present invention of ~~In a network including a centralized controller and a plurality of routers forming a security perimeter,~~ a method for selectively discarding packets during a distributed denial-of-service (DDoS) attack over ~~the~~ a network, including a centralized controller and a plurality of routers forming a security perimeter. The method includes aggregating victim destination prefix lists and attack statistics associated with incoming packets received from the plurality of routers to confirm a DDoS attack victim, and aggregating packet attribute distribution frequencies for incoming victim related packets received from the plurality of security perimeter routers.

Please amend paragraph [0013] (page 3, lines 19-20) of the specification as follows:

~~FIG. 3 depicts~~ FIGs. 3A and 3B depict a flow diagram of multi-tier Bloom filter/leaky-bucket traffic measurement arrays (BFLBAs) suitable for use in the present invention;

Please amend paragraph [0014] (page 3, lines 21-22) of the specification as follows:

~~FIG. 4 depicts~~ FIGs. 4A and 4B depict a flow diagram illustrating packet differentiation and overload control of the present invention; and

Please amend paragraph [0015] (page 3, lines 23-24) of the specification as follows:

~~FIG. 5 depicts~~ FIGs. 5A and 5B depict an illustrative flow diagram for defending against a distributed denial-of-service attack (DDoS).

Please amend paragraph [0022] (page 5, lines 16-27) of the specification as follows:

FIG. 1 depicts a schematic diagram of a network environment 100 suitable for implementing the present invention. The network environment comprises at least one client network 110 to be protected, at least one network processor (e.g., network

processors 106_1 to 106_r, where r equals and integer greater than 0, collectively network processors 106), a plurality of core routers (e.g., core routers 104_1 to $\underline{104_p}$ [[106_p]], where p equals and integer greater than 1, collectively core routers 104), at least one distributed denial-of-service control server (DCS) (e.g., DCS 108_1 to $\underline{108_q}$ [[106_q]], where q equals and integer greater than 0, collectively DCS 108), and at least one autonomous source (AS) (e.g., AS 112_1 to 112_m, where m equals and integer greater than 0, collectively AS 112), such as a server or router remotely located from the network of the victim device.

Please amend paragraph [0028] (page 7, lines 17-27) of the specification as follows:

Referring to FIG. 1, an exemplary victim server 120 of stub network 110_n is illustratively shown being attacked from a plurality of sources, illustratively, along two paths $\underline{118_1}$ [[114_1]] and $\underline{118_s}$ [[114_s]], where s is an integer greater than 1. In particular, the attacking packets from the autonomous source 112 are routed to the victim based on the victim's destination address in each packet header. For example, a first stream of attacking packets [[are]] <u>is</u> illustratively shown as being routed via the first exemplary path $\underline{118_1}$ [[114_1]], which is illustratively formed by a first source router (not shown) originating in the second autonomous system AS2 112_m, and traverses through 3D-R 106_3, core router R 104_p, 3D-R 106_r, and into the stub network 110_n, where the first attacking packet stream is received by the victim server 120.

Please amend paragraph [0029] (page 7, line 28 – page 8, line 3) of the specification as follows:

Similarly, a second stream of attacking packets [[are]] <u>is</u> illustratively shown as being routed via the second exemplary path $\underline{118_s}$ [[114_2]], which is illustratively formed by a second source router (not shown) originating at the first stub network 1 110_1, and traverses through 3D-R 106_1, core router R 104_4, core router R 104_3, 3D-R 106_r, and into stub network 110_n, where the second attacking packet stream is received by the victim server 120. Thus, the illustrative distributed attack is depicted as occurring along attack paths $\underline{118_1}$ [[114_1]] and $\underline{118_s}$ [[114_s]], such that the aggregate of the attacking packets (i.e., first and second streams) may incapacitate the victim device 120.

Please amend paragraph [0035] (page 9, line 23 – page 10, line 2) of the specification as follows:

FIG. 1 depicts the support of distributed detection and overload control by a set of 3D-Rs 106 and DCSs 108. Let r be the total number of 3D-Rs 106 along the security perimeter 114. The use of DCS 108 not only reduces the $O(r^2)$ peer communications among the 3D-Rs to $O(r)$, but it also spares the 3D-Rs 106 from the burden of managing a large number of per-end-point-target nominal traffic profiles. Since a DCS 108 exchanges only control messages with the 3D-Rs [[108]] 106 via exchange paths 116, such control messages may be kept safely away from the normal data path, i.e., out of the reach of potential DDoS attack traffic. To facilitate load balancing and improve scalability, the set of potential end-point targets within a domain may be partitioned among multiple DCSs (e.g., DCS 108_1 and DCS 108_q, where q equals an integer greater than 1.

Please amend paragraph [0045] (page 12, lines 5-11 23) of the specification as follows:

~~FIG. 3 depicts~~ FIGs. 3A and 3B (referred to collectively as "FIG. 3") depict a flow diagram of multi-tier Bloom filter/leaky-bucket traffic measurement arrays (BFLBAs) 314 suitable for use in the present invention. Referring to FIG. 3, each 3D-R 106 examines each packet header 302 of an arriving packet, classifies and measures (counts) particular parameters of the arriving packet 202, and then sends local victim IP prefix and attack statistics to the DCS 108, where the statistics are aggregated, as discussed below in greater detail with respect to FIG. 4 [[6]].

Please amend paragraph [0048] (page 12, line 30 – page 13, line 6) of the specification as follows:

Each BFLBA 314 is used to identify a list of destination networks that receive abnormally high volume of traffic compared to the leaky bucket drain rate associated with that array. Multiple instances of BFLBAs 314, each having a different leaky-bucket drain rate, e.g., 100 kbps, 1 Mbps, 5 Mbps, 10 Mbps, are used to monitor different tiers of end-points according to the nominal rate of traffic they received. The tier classification of

each end-point or stub network 110 may be based on the access link capacity of the stub network or via a periodical calibration process. Similarly, a different set of BFLBAs [[114]] 314 are set up to monitor abnormal jumps in packet arrival rates, i.e., in units of packet/sec, towards the potential victim end-points.

Please amend paragraph [0049] (page 13, lines 7-22) of the specification as follows:

As depicted in FIG. 3B ~~the lower portion of FIG. 3A~~, another set of BFLBAs 314_{t11} through 314_{t1z} (where z is an integer greater than 1) is augmented with a distinct flow identifier (DFI) 318 to determine whether an arriving packet belongs to a new or existing flow. Here, a flow is defined as a group of packets having the same 5-tuple of {source IP address, destination IP address, source port number, destination port number, and protocol type}. By passing only the first packet of each flow to the subsequent stage of BFLBAs, the DFI 318 in effect converts packet arrivals to flow arrivals. By setting the drain rate of the leaky buckets in the subsequent tiers of BFLBAs according to their nominal flow arrival rates, the destination networks that experience an abnormally high flow arrival rate may be detected. The DFI 318 also feeds its output to another set of BFLBAs 314_{t21}through 314_{t2z}, which are used for detecting possible surges of the total number of active flows carried by each end-point. For these types of BFLBA 314_{t2z}, the buckets are not drained at a constant nominal rate. Rather, flow arrival counts are accumulated within the corresponding buckets and get counted periodically.

Please amend paragraph [0056] (page 15, lines 6-17) of the specification as follows:

Alternatively, a large spike in one of the attributes from a single 3D-R 106 may be enough to conclude that an attack may be occurring. For example, a spike to 5 Mbps at AS2 112.sub.m may be deemed sufficient for the DCS 108.sub.q to conclude an ongoing attack and then proceeds to the differentiation functions [[232]] 230 and 240, as discussed below in further detail. The above example is provided for illustrative purposes only, and one skilled in the art will appreciate that other attributes (e.g., flow rate, among others) may be used instead or in conjunction with each other in a similar manner to detect a possible DDoS. For example, an ongoing attack may be said to have been detected by the DCS 108 in an instance where none of the predetermined thresholds are exceeded

individually, but collectively, the overall increase to the victim 120 exceeds some predetermined aggregate threshold.

Please amend paragraph [0062] (page 16, lines 22-25) of the specification as follows:

[0062] ~~FIG. 4 depicts~~ FIGs. 4A and 4B (referred to collectively as "FIG. 4") depict a flow diagram illustrating packet differentiation and overload control of the present invention. That is, FIG. 4 illustrates the operations between CLP computation at the 3D-Rs 106 and the determination of dynamic discarding threshold for CLP at the DCS 108.

Please amend paragraph [0077] (page 20, line 14-24) of the specification as follows:

The DCS 108 generates a scorebook for each attribute, where each attribute has an entry for each possibility. Referring to FIG. 4, two exemplary attribute scorebooks of a plurality of attribute scorebooks 416 are shown. In particular, a first exemplary attribute 418_1 for protocol type comprises a listing of the protocol types received from the current and nominal histograms (e.g., TCP, UDP, ICMP, among others), and a "score" (i.e., value) 420_1 associated with each listed protocol type. Similarly, a second exemplary attribute 418_2 (e.g., destination port) comprises a listing of the destination ports received from the current and nominal histograms (e.g., e.g., port 21, port 60, among others), and a "score" (i.e., value) ~~418_2~~ 420_2 associated with each listed destination port. Details of computing the value of each score is discussed in further detail below.

Please amend paragraph [0092] (page 24, lines 15-25) of the specification as follows:

~~FIG. 5 depicts~~ FIGs. 5A and 5B (referred collectively as "FIG. 5") depict an illustrative flow diagram 500 for defending against a distributed denial-of-service attack (DDoS). Specifically, FIG. 5 shows selective discarding of the packets generated by a SQL Slammer attack (also known as the Sapphire Worm). The attack is illustratively comprised of UDP packets with destination port number 1434, and of packet size ranging from 371 to 400 bytes. For purposes of understanding the invention, a nominal profile includes the iceberg-style histograms 502, shown therein. For example, a first nominal iceberg-style histogram 502_1 is provided for the destination port number distribution

attribute, a second nominal iceberg-style histogram 502_2 is provided for the protocol type distribution attribute, and a third nominal iceberg-style histogram 502_3 is provided for the packet size distribution attribute.